Protecting people from illegal harms online

Volume 6:
Information gathering and enforcement powers and approach to supervision

Consultation

Published: 9 November 2023
Closing date for responses: 23 February 2024

Contents

Section

27. Introduction

27.1 In this volume, we set out the powers that the Act confers on Ofcom to gather information, how we propose to use our enforcement powers, and our approach to supervision.

27.2 This volume is structured as follows:

- **Chapter 28, 'Information powers'.** The OS Act grants Ofcom powers to gather information in order to exercise our online safety duties and functions. These are explained in this chapter, along with the potential consequences for persons failing to comply with a requirement under these powers.
- **Chapter 29, 'Enforcement powers'.** This chapter covers the powers that the OS Act grants Ofcom to take enforcement action against services for non-compliance with online safety duties.
- **Chapter 30, 'Approach to supervision'**. This chapter sets out our approach to a small subset of the highest reach or highest risk services that will be in scope of the Act.

27.3 We have produced one draft guidance document to help in-scope services comply with their obligations under the Act. This is:

- **Annex 11, 'Enforcement guidance'**. Sets out guidance on how we intend to use our enforcement powers, set out in Chapter 6 of Part 7 of the Act. These powers enable us to enforce the duties and requirements applying to service providers and, where relevant, other third parties.

27.4 We are consulting on this draft guidance and have set out specific consultation questions in chapter 28 and 29 on issues where we would particularly welcome feedback. See Annexes 1-4 for more information about how to respond to our consultation.

27.5 Having reviewed responses to this consultation, we will then publish our final decisions in a Statement and our final version of this guidance document.

28. Information gathering powers

What is this chapter about?

The Act gives Ofcom the power to require information we need for purposes of exercising, or deciding whether to exercise, our online safety duties and functions. This chapter gives an overview of Ofcom's information gathering powers and Ofcom's approach to information gathering under the Act.

What are we proposing?

We will use our information gathering powers in a way that is proportionate to the use to which the information will be put and will only issue an information notice where we require information to exercise an online safety function or to decide whether to do so. We expect to use our power to issue statutory information notices regularly from the outset of the regime. Any information notices we issue will clearly set out the purpose of the request and why we require the information. We do not anticipate using our other information gathering powers such as skilled persons reports and powers of entry, inspection and audit as often, and these will typically be reserved for more serious cases.

We have lots of experience in handling information received from regulated services, and other third parties. We will not disclose confidential information unless there is a legal reason to do so, and we will carefully consider the need to disclose against any confidentiality concerns the person providing the information may have.

We expect to publish guidance on how we will use our information gathering powers at a later stage in the implementation of the Act.

Why are we proposing this?

The ability to gather information is fundamental to Ofcom being able to carry out our functions and protect users online. We will therefore use these powers where we think it is proportionate to do so.

What input do we want from stakeholders?

Do you have any comments on our proposed approach to information gathering powers under the Act?

Introduction

28.1 It is important that Ofcom's regulatory decisions are founded on a robust evidence base so that we exercise our functions under the Act in a way that is effective and proportionate. Information held by the firms that we regulate is fundamental to a proper appreciation of the factual, economic and legal context within which we exercise our regulatory functions.

28.2 The statutory information gathering powers conferred on Ofcom by the Act give us the legal tools to obtain information in support of our online safety functions. These powers will help us to address the information asymmetry that exists between Ofcom and regulated services and to discover, obtain and use the information we need, including for monitoring and understanding market developments, supervising regulated services, and investigating suspected compliance failures.

28.3 This chapter sets out a brief overview of our information gathering powers and our approach to information gathering, including our proposal to produce additional guidance on these powers at a later date.

Overview of Ofcom's information gathering powers

28.4 The Act provides Ofcom with powers to:

a) issue information notices;

b) require a report from a skilled person;

c) require an individual to attend an interview;

d) authorise persons to exercise powers of entry, inspection and audit; and

e) co-operate and share information with regulators in other jurisdictions.

28.5 These powers are briefly set out in the following sections.

Information notices

28.6 Ofcom may issue a notice (an 'information notice') to a person requiring the provision of specified information for the purpose of exercising, or deciding whether to exercise, our online safety functions. This power applies to services regulated under the Act, and also applies more widely to include:

a) a person who provides an ancillary facility[1] or an access facility[2] to a regulated service; and

b) a person who appears to us to have, or to be able to generate or obtain, information that we require, for example a related company in the same corporate group as the regulated service.

28.7 Our information notice power includes, but is not limited to, gathering information for the following purposes:

a) assessing services' compliance with relevant online safety duties and requirements;

b) consulting on a threshold figure and ascertaining the amount of a person's qualifying worldwide revenue for purpose of charging fees and imposing penalties;

c) producing and maintaining a register of regulated services;

d) deciding whether to give a notice relating to the sourcing or development of technology;

e) dealing with super-complaints;

f) preparing a code of practice or guidance in relation to online safety matters;

g) carrying out research and preparing reports in relation to online safety matters; and

[1] Under section 145(11) of the Act, a service is an 'ancillary service' in relation to a regulated service if the service facilitates the provision of the regulated service (or part of it), whether directly or indirectly, or displays or promotes content relating to the regulated service (or to part of it).

[2] Under section 147(10) a facility is an access facility in relation to a regulated service if the person who provides the facility is able to withdraw, adapt or manipulate it in such a way as to impede access (by means of that facility) to the regulated service (or to part of it) by UK users of that service.

h) complying with our duty to promote media literacy.

28.8 An information notice will specify or describe:

a) the information being requested from a provider;

b) why the information is needed by Ofcom;

c) the form and manner in which the information should be provided; and

d) the deadline by which the information should be provided.

28.9 As part of our power to issue information notices, we can request that a service enables Ofcom to remotely view information demonstrating in real time the operation of systems, processes and features used by the service, as well as to remotely view information generated in real time by the performance of a test or demonstration.

28.10 Ofcom can require the information to be provided in any form, including in an electronic form. Respondents should submit the information to Ofcom in a legible form, in the manner specified in the notice.

28.11 The power to require information does not apply to legally privileged information.

Failure to comply with an information notice

28.12 The recipient of an information notice has a legal duty to provide the requested information in accordance with the requirements of the information notice, and to ensure that the information provided is accurate in all material respects.

28.13 Ofcom may take enforcement action if services fail to respond to an information notice or provide incorrect or misleading information, which could result in a fine and a requirement to take steps to comply with the notice. Any enforcement action would be taken in line with our Online Safety Enforcement Guidance which we are also consulting on as part of this Consultation (see Annex 11). Any enforcement action taken prior to that guidance being published in final form will be taken in line with our current Regulatory Enforcement Guidelines for Investigations, as appropriate.[3]

28.14 A service commits an offence if it fails to comply with a requirement in an information notice issued by Ofcom relating to their service. It is also an offence if it:

a) knowingly or recklessly provides information that is false in a material respect;

b) intentionally provides an encrypted document to prevent us from understanding the information; or

c) intentionally prevents the information from being provided to us by suppressing, destroying or altering the information or document (or cause or permit this to happen).

28.15 If convicted of one of these offences, the Court may make an order requiring the service to comply with the information notice.

Senior manager liability

28.16 Within an information notice, Ofcom may require the service to name a relevant senior manager who may reasonably be expected to be in a position to ensure that the service complies with the requirements of the information notice. A senior manager is likely to be

[3] Ofcom, 2022. Enforcement guidelines for regulatory investigations

an individual who plays a significant role in making decisions or managing and organising the service's activities that relate to the subject matter of the information notice.

28.17 Ofcom may take enforcement action where a service fails to comply with a requirement to name a senior manager imposed in an information notice. This could lead to a fine and a requirement to comply, as set out in paragraph 28.13.

28.18 The named senior manager commits an offence if the service fails to comply with the information notice and the senior manager has not taken all reasonable steps to prevent that non-compliance. If convicted, the senior manager would be liable for a fine imposed by the Court.

28.19 The named senior manager also commits an offence if the service commits any of the offences set out on paragraph 28.14 above and the senior manager did not take all reasonable steps to prevent the offence. If convicted by a Court, the senior manager would be liable to a fine or imprisonment.

28.20 Possible defences include:

a) the individual was a senior manager for such a short time that they could not reasonably have been expected to take steps to prevent the offence;

b) the individual was not a senior manager at the time the offence occurred; or

c) the individual had no knowledge of being named as a senior manager in a response to the information notice in question.

Skilled person report

28.21 Ofcom may appoint a skilled person to provide us with a report, where we consider it necessary to assist us to:

a) identify and assess a failure, or possible failure, to comply with a relevant requirement;[4] or

b) understand the nature and level of risk of a service failing to comply with a relevant requirement, and ways to mitigate the risk (where we consider that the service in question may be at risk of failing to comply with a relevant requirement).

28.22 Ofcom is required to order a skilled persons report before deciding whether give a notice to a service requiring the service to use their best endeavours to develop or source technology dealing with CSEA content, and the requirements to be imposed by such a notice.

---

[4] In this section 'relevant requirement' means—
(a) a duty or requirement set out in any of the following— (i) section 9, 11, 26 or 28 (risk assessments); (ii) section 10 or 27 (illegal content); (iii) section 12 or 29 (children's online safety); (iv) section 14 (assessments related to the adult user empowerment duty set out in section 15(2)); (v) section 15 (user empowerment); (vi) section 20 or 31 (content reporting); (vii) section 21 or 32 (complaints procedures); (viii) section 23 or 34 (record-keeping and review); (ix) section 36 (children's access assessments); (x) section 38 or 39 (fraudulent advertising); (xi) section 65 (user identity verification); (xii) section 67 (reporting CSEA content); (xiii) section 72 or 73 (terms of service); (xiv) section 76 (deceased child user); (xv) section 78(3) or (4) (transparency reports); (xvi) section 82(2) (children's access to pornographic content);
(b) a requirement under section 84 to notify OFCOM in connection with the charging of fees (see subsections (1), (3) and (5) of that section); or
(c) a requirement imposed by a notice under section 122(2) (notices to deal with terrorism content and CSEA content).

28.23 A skilled person is someone who appears to us to have the skills necessary to provide such a report, and who is nominated or approved by Ofcom.

28.24 When Ofcom appoints a skilled person, we must notify the service about the appointment and the relevant matters to be explored in the report. Alternatively, we may give a notice to the service requiring it to appoint a skilled person to make such a report.

28.25 The service is liable for payment for the skilled person and is also under a duty to give the skilled person all such assistance as may be reasonably required to prepare the report. The duty to provide assistance applies to:

a) the service ('P');

b) any person who works now or has in the past worked for P in a relevant area;

c) any person who is providing or used to provide services to P related to the relevant matters; and

d) other providers of internet services.

28.26 Failure to comply with the duty to provide reasonable assistance to a skilled person may be subject to enforcement action by Ofcom (see Chapter 30).

Power to require interviews

28.27 Where Ofcom has opened an investigation into the failure, or possible failure, of a regulated service to comply with a relevant requirement, we may give an individual a notice requiring them to:

a) attend an interview with Ofcom at a time and place specified in the notice; and

b) answer questions and provide explanations about any matter relevant to the investigation. The individual is not required to disclose legally privileged information.

28.28 The notice must indicate the subject matter and purpose of the interview and contain information about the consequences of not complying with the notice. A copy of the notice will also be given to the regulated service. A person commits an offence if they fail without reasonable excuse to comply with a requirement to attend an interview and answer questions.

28.29 The individual may be:

a) an individual or individuals, if the regulated service is an individual or individuals;

b) an officer of the service;

c) a partner, if the service is a partnership;

d) an employee of the service; or

e) an individual who was within any of paragraphs (a) to (d) at a time to which the required information or explanation relates.

28.30 An individual complying with a requirement to attend an interview imposed under section 107 of the Act commits an offence if they knowingly or recklessly give information which is false in a material respect at an interview. If convicted of such an offence by a Court, the individual will be liable to a fine.

Powers of entry, inspection and audit

28.31 Schedule 12 of the Act gives Ofcom the power to authorise a person to:

a) exercise powers of entry and inspection without a warrant;

b) carry out audits; and

c) apply for and execute a warrant to enter and inspect premises.

Entry and inspection without a warrant

28.32 Ofcom can exercise this power if we believe the premises are being used in connection with the provision of a service, and we have given the occupier of the premises seven days' notice. The entry and inspection must happen at a reasonable hour, and these powers do not apply to domestic premises nor are they exercisable in respect of information or documents to which a claim for legal privilege could be maintained in legal proceedings.

28.33 The authorised person can:

a) enter the premises;

b) inspect the premises;

c) observe the carrying on of the regulated service at the premises;

d) inspect any document or equipment found on the premises;

e) require any person on the premises to provide any information or document that the authorised person considers is relevant to the provision of the regulated service; and

f) require any person on the premises to provide an explanation of any document, or to state where it may be found.

28.34 The authorised person may take copies of any documents found through these actions.

28.35 Ofcom may also give the service a notice requiring specified information to be provided at the inspection and setting out the consequences of not complying (see paragraph 28.43).

Audits

28.36 Ofcom may give a service an audit notice in order to assess the service's compliance with an enforceable requirement, or the level and nature of risk of non-compliance and ways to mitigate such a risk. Such a notice must be given at least 28 days before the start of the audit and must specify the timeframe for carrying out the actions required in the notice (see below), as well as setting out the consequences of non-compliance. It cannot be used to enter domestic premises and the powers cannot be exercised in respect of information or documents covered by legal privilege.

28.37 An audit notice may require the service to take any of the following actions:

a) permit an authorised person to enter and inspect specified premises;

b) permit an authorised person to observe the carrying on of the service at the premises;

c) direct an authorised person to documents on the premises that are of a specified description;

d) assist an authorised person to view information of a specified description that is capable of being viewed using equipment or a device on the premises;

e) comply with a request from an authorised person for a copy (in such form as may be requested) of the documents or information to which the person is directed or which the person is assisted to view;

f) permit an authorised person to inspect the documents, information or equipment to which the person is directed or which the person is assisted to view;

g) provide an authorised person with an explanation of such documents or information; or

h) make available for interview by the authorised person a specified number of people of a specified description who are involved in the provision of the regulated service.

28.38 Ofcom can, by giving further notice, revoke or vary the audit notice to make it less onerous. We may also require the service to pay some or all of the reasonable costs of the audit.

Warrants

28.39 Where Ofcom has reasonable grounds to suspect that a service is non-compliant with an enforceable duty, and there are relevant documents or information held at a premises, Ofcom may apply to a justice of the peace for a warrant to:

a) enter and search the specified premises;

b) inspect any documents or equipment found on the premises, or information capable of being viewed with equipment or a device on the premises;

c) require any person on the premises to give the authorised person all reasonable assistance. This may include a requirement to provide information and produce documents, and give an explanation of these;

d) require information stored electronically to be produced in a form that can be taken off the premises, and use any equipment on the premises to do this;

e) copy or seize documents, seize equipment, or open any container found on the premises; and

f) take a photograph or video recording of anything found on the premises.

28.40 Schedule 12 of the Act sets out further provisions relating to the execution of warrants, including that:

a) it must be exercised at a reasonable hour, unless the purpose of the search would be frustrated or seriously prejudiced by doing so;

b) the authorised person may use reasonable force, and may take such other persons and equipment or materials that appear necessary; and

c) if the premises are unoccupied or the owner is temporarily absent, the premises must be left as effectively secured against trespassers as they were found.

28.41 These powers cannot be used to enter domestic premises and the powers cannot be exercised in respect of information or documents covered by legal privilege.

Failure to comply with powers of entry, inspection and audit

28.42 It is an offence to:

a) intentionally obstruct a person acting under these powers;

b) fail to comply, without a reasonable excuse, with any requirement imposed under these powers; or

c) knowingly or recklessly provide information which is false in a material respect in response to a requirement imposed under these powers.

28.43 If convicted of any of these offences by a Court, a person is liable to imprisonment or a fine.

Disclosure of information

28.44 Ofcom is subject to a general restriction on disclosure of information under section 393 of the Communications Act 2003. Under this general restriction, information obtained by Ofcom in the exercise of our functions under the Act cannot be disclosed without the consent of the provider of the information in question.

28.45 Ofcom may be able to disclose information without the consent of the provider of the information where any of the exceptions listed under section 393(2) to (7) of the Communications Act 2003 apply. Such exceptions include, but are not limited to, disclosing information for the purpose of facilitating Ofcom carrying out our functions, or for the purposes of any civil proceedings brought under the Act.

28.46 The general restriction does not limit the matters that Ofcom may include or make public as part of a report made under the Act. Similarly, the general restriction does not apply to the publication of details of enforcement action or research, or other information published as part of our duties under Schedule 11 of the Act.

28.47 Those providing information to Ofcom will often regard it as confidential – that is commercially sensitive information or information relating to the private affairs of an individual - the disclosure of which may seriously and adversely affect the interests of the business or person to which it relates.

28.48 Ofcom has lots of experience in handling confidential information and is mindful of the importance of protecting it. As such, Ofcom will generally redact such information or withhold it from disclosures that we make. However, occasionally, we will consider that one of the exceptions to the general restriction on disclosure applies. When deciding whether to disclose confidential information we will carefully consider the need to disclose against any confidentiality concerns the person providing the information may have. If Ofcom is proposing to disclose information which a party considers confidential, we will provide advance warning.

Ofcom's approach to information gathering

Information notices

28.49 The Act places Ofcom under a duty to use our information gathering powers in a way that is proportionate to the use of the information being gathered. This is in line with Ofcom's regulatory principles to seek the least intrusive regulatory methods of achieving our objectives and ensure that interventions are evidence-based, proportionate, consistent, accountable and transparent in both deliberation and outcome.

28.50 The ability to gather information is fundamental to Ofcom being able to carry out its functions and to protect users online, and information notices will play a central role in this. We expect to issue information notices from the outset of the regime in order to carry out

our online safety functions. For example, we will need to issue information notices to gather the data needed to set a threshold figure and assess qualifying worldwide revenue to set up the fees regime.[5] All information notices will specify what information is required and why we need it.

28.51 We understand that many services will not have experience of responding to statutory information notices from Ofcom. As far as practicable, we will work with services to ensure that they can provide the required information accurately and by the deadline set. Where appropriate, this will include sending information notices in draft form, taking account of representations about our information notices from services, and providing non-technical and accessible explanations about the information notice process.

Other information gathering powers

28.52 In general, we do not expect to use our other information gathering powers such as skilled persons reports and powers of entry, inspection and audit as often as our information notices power, as these will typically be reserved for more serious or complex cases.[6]

28.53 We also do not anticipate that we will use these other information gathering powers in the period immediately after Royal Assent. If in that period we did need to rely upon our other information gathering powers (such as requiring a skilled person's report), we would explain our reasoning and approach on a case-by-case basis and would work with services to ensure they know how to comply.

28.54 Similar to our approach when issuing information notices, where we exercise our other information gathering powers we will take account of our general duties under section 3 of the Communications Act 2003. As such, we will ensure that our approach is proportionate by taking account of a range of factors including the size or capacity of the provider in question and the level of risk of harm and its potential severity, presented by the service in question. We will consider on a case-by-case basis if exercising these other information powers would be reasonable and proportionate, and we will follow any existing relevant guidance until such time as we produce specific guidance on how we will use these powers.[7]

28.55 We may also choose to gather information by other means. Other sources of information that we may draw from if appropriate include:

a) public sources, such as published research or openly available material on services' websites;

b) information provided informally by services, for example in the course of supervisory discussions;

c) data from complaints submitted by members of the public; and

d) information provided to us by other bodies, such as other regulators, MPs or consumer organisations.

[5] Part 6 of the Act

[6] Similarly, we do not expect to use our powers under section 101(3) to remotely view the operation of systems, processes and features, or tests or demonstrations as often.

[7] For example, this may include the Home Office Code of Practice: Powers of Entry. We will also have regard to our existing information notice guidance, although this is due for review and we plan to publish guidance on our information powers under the Act as part of the wider consultation on implementation.

29. Ofcom's enforcement powers

What is this chapter about?

This Chapter explains our general approach to regulatory enforcement, how we expect to approach enforcement under the Act and introduces our Online Safety Enforcement Guidance.

What are we proposing?

The Act grants Ofcom a range of enforcement powers and requires us to publish guidance on how we will exercise them. We are consulting on draft Online Safety Enforcement Guidance that sets out how we will normally approach enforcement under the Act. The approach has been informed by our experience and track record of enforcement in other sectors that we regulate.

We may decide to take enforcement action in the interests of citizens and consumers, for example to drive compliance, deter future wrongdoing, protect users from harm and hold wrongdoers to account. If we consider it appropriate to use our statutory enforcement powers under the Act, we will conduct an investigation into the potential breach following the processes set out in the draft Online Safety Enforcement Guidance. This may lead to us issuing a decision on whether a regulatory breach has taken place and imposing financial penalties and other sanctions.

The Act sets out which of the duties on regulated services are subject to enforcement action by Ofcom. As soon as an enforceable duty comes into effect, Ofcom may choose to use the relevant enforcement powers provided in the Act against any service that fails to comply.

Some of the duties, such as the duty to comply with information notices, came into effect at the time the Act passed. Other enforceable duties will not take effect until after Ofcom has finalised the relevant corresponding Codes of Practice or guidance in relation to those duties, or until secondary legislation has been passed.

We expect services to take action to come into compliance with the duties as soon as they take effect. For some duties, we will expect services to comply fully straight away. For example, the duty to comply with information notices, or the duties around risk assessments or child access assessments which already have built in statutory timescales for compliance set out in the Act.

We recognise that when the illegal content and child safety duties come into effect (following Codes of Practice being published), it may take some time for services to put in place all the necessary mitigations. For example, it may be reasonable for services to focus early efforts on putting in place the mitigations that are most likely to protect users from the most serious potential harms, or on mitigations that are relatively quick or simple to implement.

We will take a reasonable and proportionate approach to the exercise of our enforcement powers, in line with our general approach to enforcement and recognising the challenges facing services as they adapt to their new duties. For the illegal content and child safety duties, we would expect to prioritise only serious breaches for enforcement action in the very early stages of the regime, to allow services a reasonable opportunity to come into compliance. For example, this might include where there appears to be a very significant risk of serious and ongoing harm to UK users, and to children in particular. While we will consider what is reasonable on a case-by-case basis, all services should expect to be held to full compliance within six months of the relevant safety duty coming into effect.

Why are we proposing this?

The Act grants Ofcom a range of enforcement powers and requires us to publish guidance on how we will exercise them.

What input do we want from stakeholders?

- Do you have any comments on our draft Online Safety Enforcement Guidance?

Introduction

29.1 The Act grants Ofcom a range of enforcement powers and requires us to produce guidance for services on how we will exercise them. The Online Safety Enforcement Guidance (the 'Guidance'), attached in draft at Annex 11, sets out our proposals for how we will normally approach enforcement under the Act. The approach set out in the Guidance has been informed by our experience and long track record of enforcement work in the other sectors that we regulate.

29.2 This chapter of our consultation sets out:

a) our general approach to regulatory enforcement;

b) our proposed approach to online safety enforcement under the Act; and

c) what the draft Guidance covers, highlighting some of the novel aspects of the new regime.

Our general approach to enforcement

29.3 Ofcom's general approach to enforcement is guided by our regulatory principles.[8] We operate with a bias against intervention but with a willingness to intervene promptly and effectively when required. We will always seek the least intrusive regulatory methods to achieve our objectives and will strive to ensure that interventions are evidence-based, proportionate, consistent, accountable and transparent in both deliberation and outcome. These regulatory principles will also apply to online safety enforcement.

29.4 As the regulator of communications services in the UK, Ofcom uses a wide range of different tools to encourage, enable and enforce compliance by regulated services with their regulatory obligations. These include:

a) supporting activities such as publishing guidelines for industry, conducting research to better understand the markets that we regulate, and providing advice and education to consumers of communications services;

b) alternative tools that do not rely on legal powers, such as meetings or written communication with regulated services to discuss possible compliance issues and how they might be addressed through voluntary commitments; and

c) investigating breaches of regulatory rules using statutory enforcement powers set out in relevant legislation, which may lead to us issuing legally binding decisions on whether a

[8] Ofcom, no date. Regulatory Principles. [accessed 19 September 2023].

regulatory breach has taken place, and which may impose financial penalties and other sanctions.

Our proposed approach to online safety enforcement

29.5 As the independent regulator for online safety in the UK, Ofcom may need to take enforcement action in the interests of citizens and consumers to improve compliance, deter future wrongdoing, and protect users from harm.

29.6 However, we recognise that Ofcom's expanded remit as the online safety regulator is new territory for both Ofcom and the services that we will be regulating under the Act. Services will need time to understand the new regulations, and to assess and adapt their systems and processes to ensure they are complying with their online safety duties. We will take a reasonable and proportionate approach to the exercise of enforcement powers under the Act, in line with our general approach to enforcement and recognising the challenges facing services as they adapt to their new duties. This will be balanced against the need for Ofcom to take swift action where UK users are exposed to the risk of serious harm.

Transition periods

29.7 The Act sets out which of the duties on regulated services are subject to enforcement action by Ofcom.[9] As soon as an enforceable duty comes into force, Ofcom may choose to use the relevant enforcement powers provided in the Act against any service that fails to comply with that duty.

29.8 Some enforceable duties, such as the duty to comply with information notices, came into force at the time the Act passed. Accurate information from services is vital to enable Ofcom to exercise our regulatory functions under the Act. For example, we will need to gather information to calculate fee thresholds and to monitor implementation. We will expect services to comply fully with these duties from the outset. If a service fails to do so, for example by not responding by the deadline specified in an information notice or not providing complete and accurate information, they are at risk of enforcement action by Ofcom.

29.9 Other enforceable duties will not take effect until after Ofcom has finalised the relevant corresponding Codes of Practice or guidance in relation to those duties, or until secondary legislation has been passed. For some of these duties, the Act sets statutory timescales for services to comply. Specifically, services must carry out their first illegal content risk assessment and first children's access assessment within three months, beginning on the day on which the corresponding guidance is published. The first children's risk assessment must also be carried out within specific timescales.

29.10 Given these statutory deadlines and the importance of these assessments to enable services to understand the mitigations they need to put in place to meet their other online safety duties, Ofcom will expect all services to comply fully with these duties by the statutory deadline. We may decide to take enforcement action if these assessments are not completed within the period set out in the Act.

29.11 We recognise that when the illegal content and child safety duties come into effect (following publication of the relevant Codes of Practice), it may take some time for services

[9] A table of enforceable duties is set out at section 131(2) of the Act.

to bring themselves fully into compliance. For example, it may be reasonable for services to focus early efforts on putting in place the mitigations that are most likely to protect users from the most serious potential harms, or on mitigations that are relatively quick or simple to implement.

29.12 We therefore acknowledge that services may require a reasonable period to put in place appropriate systems and processes to bring them into full compliance with these duties. This is likely to particularly be the case for smaller services and those new to regulation. These services may not have existing systems that could be adapted to meet their online safety obligations, needing a longer preparation period, and may not have the resources available to larger services. Our focus in the early regulatory period will be on working with services to help them understand their obligations and any steps that are needed for them to come into compliance.

29.13 We will take these challenges into account when considering whether it is appropriate to take enforcement action against non-compliance with the illegal content and child safety duties. We would expect to prioritise only serious breaches of these duties for enforcement action in the very early stages of the regime, to allow services a reasonable opportunity to come into compliance. For example, this might include where there appears to be a very significant risk of serious and ongoing harm to UK users, and to children in particular.

29.14 While we will consider what is reasonable on a case-by-case basis, all services should expect to be held to full compliance within six months of the relevant duty coming into effect.

29.15 This phased approach means that we expect Ofcom's enforcement action to increase over time as the regime comes into effect, although we remain ready to take early action as necessary and appropriate.

Online Safety Enforcement Guidance

29.16 We are proposing standalone Guidance so that there is clarity for newly regulated services about our enforcement procedures under the Act. We will follow our Regulatory Enforcement Guidelines[10] to the extent relevant if we take enforcement action under the Act prior to the publication of the Guidance in final form following consultation.

29.17 The proposed Guidance is divided into ten sections:

i) Overview
ii) Introduction
iii) Enforcement action and when we use it
iv) Initial assessment of the issues
v) Opening an investigation and information gathering
vi) Determining the outcome of our investigation
vii) Liability of Related Entities and Controlling Individuals
viii) Settlement Procedure
ix) Business Disruption Measures
x) Procedural complaints about investigations

[10] Ofcom, 2022. Regulatory Enforcement Guidelines for investigations. [accessed 19 September 2023].

29.18 This chapter of our consultation highlights our proposals in relation to some of the novel aspects of enforcement under the new regime, as set out in sections iii, vi, vii and ix. Information gathering powers (bullet v above) are covered in Chapter 28.

When we may take enforcement action

29.19 This section of the draft Guidance focuses on how and when Ofcom may decide to take enforcement action. It sets out our principal duties and objectives, as well as other matters to which we must have regard. It also explains some of the ways in which Ofcom may become aware of potential compliance issues and the range of enforcement tools that we might consider in response to these issues, including non-statutory alternative enforcement tools.

29.20 We cannot pursue enforcement action against every potential compliance issue. We propose to consider the priority factors listed in the Guidance when making decisions about whether to take enforcement action. These relate to:

a) the risk of harm or seriousness of the alleged conduct and any impact this may have on the risk of harm presented by content available on the regulated service;

b) the strategic significance of addressing the conduct; and

c) the resource implications and risks in taking enforcement action.

29.21 These factors are explained in more depth in the draft Guidance. Not all factors will be relevant to every potential issue, and we will consider the factors in the round depending on the circumstances of the particular issue we are considering.

Prioritisation and the risk of harm to children

29.22 The newly amended section 3(4A) of the Communications Act requires us to have regard to, among other matters, the need for a higher level of protection for children than for adults. Section 151(3) of the Act also states that our enforcement guidance must include an explanation of how we will take account of the impact (or possible impact) of non-compliance on children.

29.23 We propose to include the harm or risk of harm to children in our prioritisation framework when considering:

a) the risk of harm or seriousness of the conduct; and

b) the strategic significance of addressing the alleged contravention.

29.24 Including the risk of harm to children in two parts of Ofcom's prioritisation framework reflects the importance of this factor in considering whether or not to take enforcement action.

Prioritisation and content

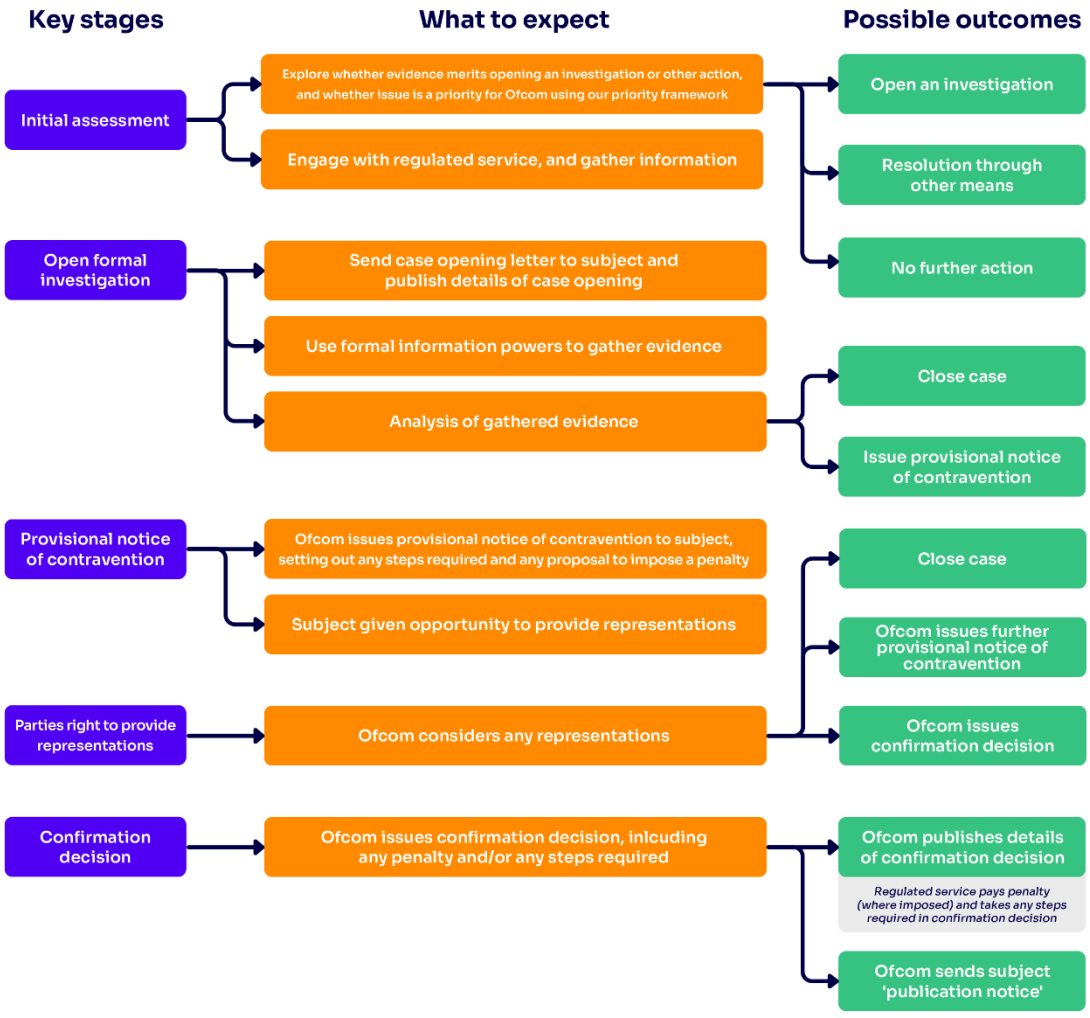
29.25 The online safety regime is focused on the online safety systems and processes of services in scope of the Act and is not about regulating individual pieces of content found on these services. The presence of illegal content, or content that is potentially harmful to children, does not necessarily mean that a service is failing to fulfil its duties in the Act. We would not therefore necessarily take enforcement action solely based on evidence of harmful content appearing on a service.

29.26 However, evidence of especially harmful material or the prevalence of harmful material on a service (particularly if it is on a service for a prolonged period of time without being removed or presents a particular risk to children because of the type of regulated service on which it appears), would be a potential indicator that a service's systems and processes were insufficient to protect users from such content. This may be relevant to our assessment of whether the issue is a priority for Ofcom such that enforcement action may be taken following our investigation of the issue.

Determining the outcome of a compliance investigation

29.27 This section of the draft Guidance sets out our proposals about how Ofcom will decide on the outcome of an investigation into potential compliance issues, and who will make the key decisions. The Guidance explains the stages of the decision-making process including the decisions to issue a provisional notice of contravention, and then whether to issue a confirmation decision where we are satisfied there has been a contravention; we summarise these below. Figure 29.1 provides an overview of the possible outcomes of an investigation.

Figure 29.1. Possible outcomes of an investigation



Source: Ofcom

Deciding whether to issue a provisional notice of contravention

29.28 Following an investigation, we may decide to:

a) close the investigation without issuing a provisional notice of contravention against the service. In most cases we will publish on our website a brief statement indicating case closure and the basis for doing so, usually after first informing the subject of the complaint and any complainant of our decision; or

b) issue a provisional notice of contravention, if we consider there are reasonable grounds for believing that the subject of the investigation has failed, or is failing, to comply with one or more online safety duties.

Issuing a provisional notice of contravention

29.29 Ofcom may issue a provisional notice of contravention where we consider there are reasonable grounds to believe that the subject of an investigation has failed, or is failing, to comply with one or more of its obligations.

29.30 The provisional notification will be sent to the service. Occasionally we may also provide complainants or third parties with an opportunity to comment on a non-confidential copy of the notification. The notification will set out:

a) the safety duties or obligations in question, the period over which the alleged failure(s) have occurred, and the reasons for Ofcom reaching its provisional finding;

b) any proposed financial penalty and why we consider it to be appropriate; and

c) any further steps we consider the service should take to comply with and/or remedy the proposed contravention(s) and the reasons we believe these to be appropriate.

29.31 We will not publish provisional notices of contravention, but we will generally publish an update on our website to note that one has been issued.

Representations on the provisional notice of contravention

29.32 When we issue the provisional notice of contravention, we will also provide the service with copies of, or access to, the evidence on which we have relied in reaching our provisional view. The subject will have the opportunity to make representations on our proposed findings before we proceed to the next stage of the investigation, either as written representations or at an oral hearing. More details about the process for this are set out in section 6 of the draft Guidance.

29.33 In some cases, new information may come to Ofcom's attention after we have issued a provisional notice of contravention and the service has submitted written or oral representations. We will adopt an appropriate process to deal with any new evidence which ensures fairness to the subject of the investigation. As a result of this we may choose to withdraw the initial provisional notice and either issue a further provisional notice of contravention or, alternatively, we may decide to close the case.

Decision to issue a confirmation decision

29.34 Having considered all the relevant evidence and any written representations we may decide to close the investigation at this stage. Alternatively we may proceed to issuing a confirmation decision if we are satisfied that the service has failed, or is failing, to comply

with one of more of its obligations. The confirmation decision will confirm this finding, and set out:

a) our reasons for reaching that conclusion and the evidence on which we have relied;

b) any financial penalty; and

c) steps the subject of the investigation is required to take to come into compliance, and/or remedy the failure with the duty or duties.

29.35 Once Ofcom has notified the subject of the investigation of our findings and issued the confirmation decision and any penalty notices (see paragraph 29.35 below), we will close the investigation and publish this fact on our website. As soon as possible after we have closed the investigation, we will also publish a non-confidential version of the confirmation decision on our website.

Financial penalties

29.36 Ofcom may impose a financial penalty of up to 10 percent of qualifying worldwide revenue or £18 million (whichever is the greater) in respect of a contravention if we consider that appropriate and proportionate, taking account of the circumstances in the round. Any penalty that we impose will be set in accordance with our published Penalty Guidelines.[11] For online safety enforcement, we will specifically take account of the harm or risk of harm to children in determining any penalty amount.

29.37 A financial penalty may be a single penalty, a daily penalty where the contravention is still ongoing, or a combination of the two. So far as it is relevant, Ofcom will follow the same procedures as for a provisional notice and confirmation decision, such that the service will have the opportunity to make representations on the penalty notice.

Requirement to take steps

29.38 Ofcom can require a service to take specific steps in relation to UK users where we have found it has breached one or more of its obligations, either to bring the service into compliance and/or to remedy the failure to comply.

29.39 For breaches of certain obligations there are specific actions that Ofcom can require a service to take:

a) breach of the risk assessment duty: Ofcom can require the service to take steps to mitigate any risks that Ofcom has identified, despite the service itself not having identified the risk in its risk assessment.

b) breach of the duties about children's access assessment: Ofcom can require a service to carry out or repeat its children's access assessment. Where we determine that it is possible for children to access all or part of the service and the child user condition in section 35(3) of the Act is met,[12] we can also set out the circumstances in which this determination will cease to apply – for example, if the service were to implement age verification.

[11] Ofcom, 2017. Penalty Guidelines (as amended). [accessed 19 September 2023].

[12] The child user condition is met if either: (a) a significant number of children are users of the service, or part of the service; or (b) the service, or part of it, is likely to attract a significant number of child users.

Consequences of continued non-compliance

29.40 Where a deadline for compliance with the required steps set out in the confirmation decision is not met, or where Ofcom finds that a service has not fully complied with the required steps, we may issue a penalty notice requiring the service to pay a financial penalty.

29.41 A penalty notice may also be triggered by a failure to comply with a notice to deal with terrorism and CSEA content under section 121 of the Act,[13] or a failure to pay a fee set under section 84 or Schedule 10 of the Act.[14]

Liability of Related Companies and Controlling Individuals

29.42 In certain situations, Ofcom may issue a provisional notice of contravention and a confirmation decision to both the service and another entity related to the service. Where we do so, the related entity will be jointly and severally liable with the service for any contravention by that service that we find in a confirmation decision.

29.43 An entity will be related to a regulated service where it is:

a) a parent company;

b) a subsidiary company;

c) a fellow subsidiary entity (with the same parent company as the regulated service); or

d) a person or persons who control the company that provides the service.

29.44 We refer to categories a) – c) as a 'Related Company' and category d) as a 'Controlling Individual'. These relationships are described in more detail in the draft Guidance in section 7.

29.45 As set out in the draft Guidance, we are proposing that it may be appropriate to pursue a Related Company or Controlling Individual, in addition to the service, to better meet our objectives of deterrence and incentivising compliance where we have grounds to believe that:

a) the Related Company or Controlling Individual had some responsibility for the failure under investigation. A Related Company which qualifies as a parent company or a Controlling Individual will usually meet this threshold by virtue of its control of the regulated service; or

b) any enforcement action we take may be more effective if a Related Company or Controlling Individual has joint and several liability with the service.

29.46 We also propose to take account of our prioritisation framework when considering whether to pursue enforcement action to make a Related Company or a Controlling Individual jointly and severally liable for any contravention that we find by a regulated service.

29.47 We set out in the draft Guidance process we propose to follow when taking enforcement action against a Related Company or Controlling Individual. Where we decide to do so before issuing a provisional notice of contravention to the service, generally we propose to

[13] Section 140 of the Act.
[14] Section 141 of the Act.

involve the relevant Related Company or Controlling Individual throughout the investigation process.

29.48 We are also empowered to issue such a notice or confirmation decision to a Related Company or Controlling Individual after finding a contravention by the service in a confirmation decision. As set out in the draft Guidance, this may be appropriate where additional evidence has come to our attention at a late stage in the process or there is a change in circumstances which gives us cause to reassess the effectiveness of our enforcement action against the service.

29.49 Where a penalty has been issued jointly with a Related Company or Controlling Individual, the maximum penalty Ofcom may impose on the service and the Related Company or Controlling Individual is whichever is the greater of:

a) £18 million; and

b) 10 percent of the qualifying worldwide revenue of the group of companies that consists of:

i) the company that provides the online service; and
ii) every other company which, at the time the decision or notice is given, is in the same company group as the company providing the online service.

Business Disruption Measures

29.50 Business disruption measures are orders made by a Court on an application from Ofcom. They apply to third parties which are in a position to take action to disrupt the business of a service and thereby reduce the risk of harm to UK citizens and consumers. It is the decision of the court whether to grant any such application by Ofcom.

29.51 There are four types of business disruption measures.

a) **Service restriction orders** require 'ancillary providers', such as search engines and payment services which facilitate the provision of the service, to take steps aimed at disrupting the non-compliant service's business in the UK. For example, search engines may be required to remove a non-compliant provider from its search results.

b) **Interim service restriction orders** are similar to service orders but are made on a temporary basis. The court must be satisfied that the service is likely to be non-compliant and that the resulting level of risk of harm, and the nature and severity of that harm, are such that it would not be appropriate to wait to establish the failure to comply before applying for the order.

c) **Access restriction orders** require a service which enables access to a service, such as an internet access service or an app store, to take steps to restrict access to a non-compliant provider, for example, by removing its app from the app store. These orders can be applied for by Ofcom if we consider that a service restriction order or an interim service restriction order has not proved sufficient to prevent significant harm to individuals in the UK from the contravention in question or would be unlikely to do so.

d) **Interim access restriction orders** are similar to access restriction orders but are made on a temporary basis, if the court is satisfied that the service is likely to be non-compliant and that the resulting level of risk of harm, and the nature and severity of that harm, are such that it would not be appropriate to wait to establish the failure to comply before applying for the order.

29.52 As set out in the draft Guidance, when deciding whether it is appropriate to seek business disruption measures, we propose to do so in line with our regulatory principles and only where we consider it would be proportionate in the circumstances. We must consider, as a minimum, that there is a continuing failure to comply or that it is likely that there is or will be such a failure. Where this is the case, we propose to take account of our priority framework when deciding whether to make an application. In particular, we propose to consider the level and degree of any risk of harm to individuals in the UK from the failure we have identified, including whether there is actual or potential harm to children, and whether there are other steps that are likely to achieve the same ends or deal with the same issues as a business disruption measure.

29.53 We do not consider it would be appropriate to apply to the Courts for business disruption measures as matter of routine where we have identified failures to comply with enforceable requirements. In the draft Guidance, we propose some examples of circumstances in which we may consider it appropriate, including:

a) where a service has failed to take the required steps imposed by a confirmation decision, and has failed to engage with Ofcom in relation to coming into compliance; or

b) where a service has a history of failure to comply with required steps or penalties, such that we consider that use of other enforcement tools would be unlikely to be effective.

29.54 Where possible we propose to engage with the third parties who may be the subject of a business disruption measure before making an application to Court for such an order. This may not be possible in every case, and the draft Guidance provides some examples.

29.55 Once Ofcom has decided to make an application for business disruption measures, the rest of the process is governed by the procedural rules applicable in the relevant Court. Ofcom is not able to offer guidance or advice on the Court process and potentially affected parties should take their own legal advice in relation to this.

Impact assessment

29.56 Generally, Ofcom will not conduct an impact assessment when publishing guidance relating to how we undertake enforcement action. The draft Guidance on which we are consulting describes the procedures that we will follow when taking enforcement action against non-compliant regulated providers. These powers, and the enforceable duties, are contained in the Act, and have been subject to impact assessments through the legislative and policy making process.

29.57 Ofcom does have discretion in deciding whether and how to act, such as whether to open an investigation, take informal action or apply to the Court for business disruption measures. In taking these decisions we will be guided by our regulatory principles and the priority framework set out at paragraphs 3.8 – 3.10 of the Guidance, which direct enforcement action towards the most significant cases, according to:

a) the risk of harm or seriousness of the alleged conduct or contravention;

b) the strategic significance of addressing the alleged contravention; and

c) the resource implications and risks in taking enforcement action.

29.58 Providing transparency about the factors that inform the exercise of our discretion creates certainty and may encourage appropriate investment by services. Clarity about when

enforcement action is likely incentivises compliance, deters future wrongdoing, and protects users from harm.

30. Supervision

What is this chapter about?

This chapter sets out our approach to supervision of a small subset of the highest reach or highest risk services in scope of the Online Safety Act. Supervision will help ensure that these services have appropriate systems and processes to achieve the key outcomes intended by the Act to make life safer online for people across the UK.

Introduction

30.1 In this chapter we cover Ofcom's approach to online safety supervision. We describe the principles behind our approach; what we aim to achieve through supervision; the types of services we will supervise; how we will supervise those services; and the difference between supervision and enforcement. We also cover our approach to how we will engage with services we will not supervise.

30.2 The UK Online Safety Act 2023 ('the Act') makes a wide range of online services (including user-to-user services, search services and pornography services[15]) legally responsible for keeping people, especially children, safe online. As stated in the background document[16] published alongside this consultation, the onus is on services to determine what measures they need to put in place, given the risks they face.

30.3 We know that many services may need to make significant changes to how they operate, including investing in new safety measures to protect users. We therefore want to engage closely with certain services to understand the risks that could harm users, assess the effectiveness of their safety measures and work with the service to secure improvements where necessary. As a result, we are proposing to adopt a proportionate 'supervisory' approach, focusing on services that represent the highest reach or highest risk of harm to ensure we are focusing our resources on those services capable of having the greatest impact.

What is supervision?

30.4 Supervision is an approach used in some regulated sectors to oversee how an organisation complies with a set of rules or legislation and, in some cases, ensure user safety. Given the remit of the Act, Ofcom has decided to adopt a supervisory approach that builds on Ofcom's experiences of developing supervisory relationships with the video sharing platforms we already regulate, which has been helpful in understanding those services and in securing improvements to keep users safe. In this instance, the term 'supervision' describes a set of activities to manage Ofcom's relationships with services to understand and mitigate future risks and secure improvements in Ofcom's focus areas of Governance, Design and Operations, Choice and Trust (set out in Ofcom's approach to implementing the Online

[15] See Ofcom's approach to implementing the Online Safety Act for more detail on which services will be covered by the legislation.
[16] See Ofcom's approach to implementing the Online Safety Act.

Safety Act[17]). Supervision will also address the key harms (as listed in the Act) of child sexual exploitation and abuse; online terrorism and hate; and fraud and scams.

30.5 In line with the wider approach to delivering online safety, supervision will focus on the effectiveness of services' systems and processes in protecting their users, not on individual pieces of content. We will aim for as much consistency in our approach across services as possible, while tailoring discussions where appropriate according to a service's particular needs. Our supervisory approach will be flexible, proactive, proportionate, risk-based and align with Ofcom's aim to embed our standards, identify opportunities for improvements and drive these improvements.

Why are we supervising certain services?

30.6 Our ambition is to drive change for all users of all online services. However, we cannot proactively engage with every service that is within scope of the Act. By focusing our resources on the most 'impactful' services, we hope to (a) improve safety for the users of that service – which may be a significant user base/proportion of online users/UK users and (b) establish baseline standards, which will help to bring up standards across the rest of the industry.

30.7 We believe a supervisory approach will be an effective and appropriate way to achieve our aims. In some circumstances, potentially because of their commercial objectives, certain services may consider improvements that go above and beyond the approaches we have set out in our Codes of Practice for the benefit of their users. This in turn may help us to drive up standards across the industry.

Timely and efficient impact

30.8 Supervision will allow us to understand services and the measures they deploy to keep users safe; to assess the effectiveness of these measures in the context of the specific risks presented by that service; and to engage quickly to encourage improvements where they are proportionate and achievable. This will enable us to take prompt and effective action to mitigate risks to users – and where we identify compliance concerns that cannot be addressed through a supervisory approach we will be able to refer these to formal enforcement investigation where appropriate.

Promoting good practice

30.9 Supervision will allow us to test where it may be proportionate and feasible for services to go further than the recommended steps set out in our Codes of Practice. This in turn may help us to drive up standards across the industry. We will also be able to promote good practice across the sector by reporting on our experiences of engaging with supervised services.

Deepening Ofcom's understanding of the services we regulate

30.10 By developing a more detailed understanding of supervised services we can improve our understanding of current and emerging areas of harm, measures to address them, and provide a feedback loop for how Ofcom's regulation should develop in future. It will also

[17] See Ofcom's approach to implementing the Online Safety Act published alongside this consultation.

allow us to deepen our understanding of issues of how to strike the balance between user safety and any impacts on user rights such as freedom of expression or privacy.

Who will be supervised?

30.11 We have decided to focus our supervision on the highest reach or highest risk services – in other words, those services that are likely to have the greatest impact on users' safety. Given the number of services in scope of the Act, we are adopting a proportionate approach, as it would not be feasible to have a meaningful supervisory relationship with every regulated service. In deciding which services to supervise, we will consider factors such as: the size and reach of the service; the level of potential risk associated with the service's primary functionalities; and whether the activities and characteristics of a service present a significant risk to our priority harms, namely child sexual exploitation and abuse; online terrorism and hate; and fraud and scams.

30.12 While some factors such as size and reach can be measured, we will also need to rely on our expert judgement when deciding where to prioritise our supervisory engagement. As this is a complex and novel regulatory regime, the services we supervise will be regularly reviewed, including by reference to the information we have obtained from regulated services and other sources of evidence we may gather. We will inform services when they become supervised or are no longer supervised following our review of services.

30.13 For services that are not actively supervised we will continue to review their activities and engage with them in other ways to promote understanding of, and compliance with, this new online safety regulation (see below).

How will we supervise services?

30.14 We will have regular engagement with supervised services, with a preference for informal intervention.

30.15 In our first year, we expect to engage in regular meetings with supervised services and establish collaborative relationships with the relevant individuals and teams to build our understanding of the services and the markets within which they operate. As our relationships with supervised services develop, and more duties under the Act come into force, we expect our supervisory engagement to evolve further as we look to encourage compliance, share good practice and drive improvements across industry.

30.16 For each supervised service we intend to set supervisory strategies based around Ofcom's online safety focus areas. These will vary by service and will evolve over time, but in the initial period we would expect supervisory strategies to focus on:

- understanding the service and its business model;
- understanding existing safety measures;
- understanding governance and risk processes and assessing preparedness for risk assessment requirements under the Act; and
- reviewing approaches to tackling priority harms, including CSEA, fraud and hate & terror; and assessing age assurance (where appropriate).

Figure 30.1. Aims of our supervisory engagement

Source: Ofcom

30.17 As set out in Ofcom's approach to implementing the Online Safety Act the 'approach to regulation' background document , our approach to supervision will be underpinned by the relevant powers in the Act including statutory information gathering powers, which we will deploy proportionately. Our experience from VSP regulation is that a range of services will engage constructively and openly with us.

How will Ofcom engage with services that are not actively supervised?

30.18 As part of our focus area to build trust in the new regulatory framework and achieve change, we want to support all in scope services to be compliant with the provisions of the Act, not only those who we will actively supervise. This is particularly important for the large and diverse range of specialised services which are likely to be within scope of the Act.

30.19 As we consult on our first policy documents, codes and guidance, we are also undertaking research to understand the needs of the different types of services within scope of the regulation and will be taking an iterative approach to providing support to this diverse market. We want to understand how we can best support regulated services and drive improvements, and are exploring a range of techniques from digital tools and easy-to-use resources, to communications and engagement (both directly and through industry bodies).

30.20 We have published some initial supporting resources for services to explain the requirements of the Act. We invite all services to register for email updates so they can stay up to date on the regulation and on any new resources or tools that we make available. Feedback from regulated services will be vital to this process, so we can ensure that any new tools are effective, that regulated businesses understand what they need to do, and we can better protect users of online services in the UK.

How will supervision differ from enforcement?

30.21 Our supervision activities are separate to our enforcement processes (see Chapter 29). Our supervisory approach is intended to enable Ofcom to understand services' systems and processes for keeping their users safe, and to work with the services to secure improvements in those measures where necessary. By contrast, our enforcement powers are likely to be used where it is in the interests of citizens and consumers to address non-compliance, deter future wrongdoing, protect users from harm and/or hold services to account for failures to comply with their duties.

30.22 It is possible that our supervisory activity identifies potential compliance concerns relating to the requirements under the Act. Where potential compliance issues are identified, we

expect services to engage constructively and openly with Ofcom and be willing to make improvements. We will generally seek to resolve issues constructively with services (including non-supervised services) without pursuing formal enforcement action, as this can provide the quickest and most efficient route to ensuring users are protected from harm.

30.23 However, where we do identify serious compliance concerns or the service is not willing to engage constructively with us, we will consider whether it is appropriate to pass the issue to our Enforcement team, depending on the severity of the issue and the engagement from the service. We will use our enforcement powers where we consider it appropriate, reasonable and proportionate to do so, guided by our regulatory principles. Our approach to investigating compliance concerns and enforcing the requirements of the Act is set out in our Online Safety Enforcement Guidance, on which we are also consulting (see Annex 11).

30.24 We will inform services (whether supervised or not) whenever they become subject to a formal enforcement process.

How does supervision differ from categorisation?

30.25 Under the Act, certain categories of services will be required to comply with additional duties, such as transparency reporting and preventing fraudulent advertising. The thresholds used to determine which services are categorised will be set by the Secretary of State with reference to user numbers and functionality. While there will be some overlap between supervision and categorisation, the criteria for deciding who we will supervise are not wholly based on categorisation.

30.26 As the approaches to both categorisation and supervision develop, we will aim for a coherent approach across both processes where possible. We will keep our stakeholders informed as these two processes develop further.